Infraestrutura de Chaves Públicas Brasileira

CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DE LABORATÓRIOS DE ENSAIOS E AUDITORIA INTEGRANTES DA ICP-BRASIL

DOC-ICP-10.07

Versão 1.0

01 de outubro de 2010

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Instrução Normativa nº 08, de 01.10.2010 (Versão 1.0)		Aprova a versão 1.0 dos Critérios e Procedimentos para Credenciamento de laboratórios de Ensaios e Auditoria Integrantes da ICP-Brasil.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC-Raiz	Autoridade Certificadora Raiz
APF	Administração Pública Federal
CATI	Comitê da Área de Tecnologia da Informação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
FGTS	Fundo de Garantia por Tempo de Serviço
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ITI	Instituto Nacional de Tecnologia da Informação
LEA	Laboratório de Ensaios e Auditoria
MCT	Manual de Condutas Técnicas
PCN	Plano de Continuidade do Negócio
PS	Política de Segurança
SICAF	Sistema Unificado de Cadastramento de Fornecedores
WEB	*World Wide Web*

1. INTRODUÇÃO

Este documento estabelece os critérios e procedimentos a serem observados para o credenciamento, manutenção do credenciamento e descredenciamento de Laboratórios de Ensaios e Auditoria - LEA, no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

2. CREDENCIAMENTO

2.1. Critérios

Os LEA deverão ser entidades com capacidade técnica necessária à boa condução das avaliações de conformidade de sistemas e equipamentos de certificação digital, devendo ter sede administrativa localizada no território nacional, ter instalações operacionais e recursos de segurança física e lógica, compatíveis com as atividades de ensaios e auditoria localizadas no território nacional e atender aos procedimentos e requisitos de Qualificação Jurídica, Qualificação como Instituição de Pesquisa e/ou Laboratório, Capacidade Técnica, e Capacidade de Tratamento Sigiloso de Informações estabelecidos no DOC ICP 10, bem como os descritos neste documento.

2.2. Procedimentos para credenciamento de LEA:

2.2.1. Diretrizes Gerais

2.2.1.1. O processo de credenciamento obedece a procedimentos específicos, relacionados com a natureza da atividade a ser desenvolvida no âmbito da ICP-Brasil.

2.2.1.2. O deferimento do pedido de credenciamento será publicado no Diário Oficial da União e importará a autorização para funcionamento no âmbito da ICP-Brasil.

2.2.2. Solicitação

2.2.2.1. As solicitações dos candidatos ao credenciamento como LEA na ICP-Brasil serão encaminhadas, ao ITI mediante a apresentação dos documentos a seguir relacionados:

a) Formulário **SOLICITAÇÃO DE CREDENCIAMENTO DE LABORATÓRIO DE ENSAIO E AUDITORIA ADE-ICP-10.07.A [6]**, devidamente preenchido e assinado pelos representantes legais do candidato ;
b) documentos relacionados no Anexo I;
c) identificação do local onde será guardada a documentação e materiais utilizados nos ensaios realizados pelo LEA;
d) relatório final[1] de auditoria pré-operacional do LEA, realizada observado o disposto no ANEXO II - REQUISITOS MÍNIMOS DE SEGURANÇA PARA LABORATÓRIO DE ENSAIO E AUDITORIA;
e) identificação do serviço de diretório ou pagina web onde-se obtem o arquivo

[1] Relatório final é aquele emitido quando a auditoria não detectar não-conformidades ou quando as não-conformidades em relatório preliminar já estiverem regularizadas e certificadas pela empresa que realizou o trabalho de auditoria.

com a publicação da Política de Segurança-PS, e a relação dos sistemas e Equipamentos de Certificação Digital para os quais está credenciado junto a ICP Brasil;

2.2.2.2. A solicitação de credenciamento será protocolada perante o Protocolo-Geral do ITI e recebida, em até 30 (trinta) dias, por intermédio de despacho fundamentado.

2.2.2.3. Caso a solicitação de credenciamento não contenha todos os documentos relacionados no Anexo I, o ITI determinará a intimação do candidato para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado, pelo ITI com comprovação de recebimento pelo destinatário.

2.2.2.4. Fica dispensada a apresentação do relatório de auditoria pré-operacional se o candidato enquadra-se no item 1.d) do anexo I.

2.2.3. Auditoria

2.2.3.1. Após a publicação do despacho de recebimento, a Diretoria de Auditoria, Fiscalização e Normalização examinará a documentação apresentada e poderá, caso julgue necessário, no prazo máximo de 30 (trinta) dias:

a) solicitar vista do material utilizado na auditoria (documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração do relatório);
b) exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata; ou
c) realizar auditoria pré-operacional por seu quadro próprio, elaborando relatório que prevalecerá sobre o apresentado pela candidata.

2.2.3.2. Com base no relatório final de auditoria, o ITI manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento.

2.2.3.3. Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo do candidato ao Comitê Gestor da ICP-Brasil.

2.2.4. Ato de credenciamento

2.2.4.1. O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado ao LEA que deu encaminhamento ao requerimento.

2.2.4.2. O LEA que estiver credenciado para um determinado tipo de sistema ou equipamento fica dispensada de novo credenciamento.

2.2.4.3 O ato de credenciamento será publicado no Diário Oficial da União e condicionara a AC Raiz e o LEA, por seus representantes legais, a firmarem por meio de Termo de Acordo, onde deverá conter as responsabilidades e compromisso por parte do LEA, de que desempenharão suas funções de acordo com padrões de idoneidade que asseguram a independência e neutralidade de suas avaliações bem como o devido rigor técnico e operacional.

2.2.5. Vedações ao credenciamento

É vedado a contratação, sub contratação ou terceirização total ou parcial das atividades de ensaios e auditoria pelos LEA credenciados no âmbito da ICP Brasil, entretanto é permitido ao LEA a contratação temporária de técnicos especialistas em ensaio e auditoria, desde que seja totalmente independente do interessado na emissão do laudo de conformidade, e que não preste serviços a empresas fornecedoras de soluções iguais ou similares aos sistemas e equipamentos de certificação digital.

3. MANUTENÇÃO DO CREDENCIAMENTO

As entidades credenciadas deverão manter atendidos os critérios definidos no item 2.1, e estão sujeitas aos **CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2]** e aos **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].**

3.1 Manutenção de credenciamento de LEA

A entidade credenciada para desenvolver as atividades de LEA deverá:

a) comunicar, desde logo, ao ITI:
   i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;
   ii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil,
b) Alteração na sua Política de Segurança – PS;
c) encaminhar ao ITI, até o dia 15 (quinze) de dezembro de cada ano, cronograma das auditorias a serem realizadas, durante o ano seguinte;
d) encaminhar ao ITI relatórios de auditorias em até 30 (trinta) dias após a conclusão das mesmas.
e) observar os MCT Vol I e Vol II, e a PS aplicável;

4. DESCREDENCIAMENTO DE LEA

4.1. Hipóteses para o descredenciamento de LEA

a) A pedido do próprio LEA, mediante requerimento, em relação às suas atividades;
b) Por determinação da ITI, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.2. Procedimentos para descredenciamento de LEA

4.2.1. Descredenciamento solicitado pelo próprio LEA

Na hipótese de o descredenciamento ser solicitado pelo próprio LEA, o mesmo comunicará, com 60 (sessenta) dias de antecedência, diretamente ao ITI e aos Titulares dos Sistemas e Equipamentos de Certificação Digital para os quais foram emitidos Laudos de Conformidade para pleitearem homologação junto à ICP Brasil, e publicará em sua página *web*, para conhecimento, a decisão de encerrar suas atividades de ensaio e auditoria no âmbito da ICP-Brasil.

4.2.2. Descredenciamento por determinação do ITI

Na hipótese de descredenciamento por determinação do ITI, o LEA descredenciado fica impedido de apresentar novo pedido de credenciamento pelo prazo de 12 (doze) meses contados da publicação de que trata o item 2.2.4.3.

4.2.3. Descredenciamento por qualquer das hipóteses previstas

Em qualquer das hipóteses de descredenciamento de LEA deverão ser obedecidos os seguintes procedimentos:

a) o ITI divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página WEB;
b) O LEA deverá cessar, suas atividades de ensaio e auditoria no âmbito da ICP Brasil imediatamente após a comunicação de que trata a alínea anterior;
c) Os documentos e materiais utilizados no ensaios e auditoria relativos aos sistemas e equipamentos objeto de Laudo de Conformidade para fins de homologação junto à ICP Brasil deverão ser armazenadas por outro LEA credenciado, após aprovação da ITI;
d) Quando houver mais de uma LEA interessado, assumirá a responsabilidade do armazenamento aquele indicado pelo LEA que encerra as suas atividades;
e) Caso os documentos e materiais de posse e guarda do LEA descredenciado não tenham sido assumidos por outra LEA credenciado, os mesmos serão repassados ao ITI.

4.4. Obrigações Subsistentes

O LEA, têm o dever de observar as diretrizes e normas técnicas da ICP-Brasil, inclusive as obrigações que subsistirem após o encerramento das atividades de ensaio e auditoria.

5. DOCUMENTOS REFERENCIADOS

5.1. Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que

os aprovaram.

Ref	Nome do documento	Código
[1]	**CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL**	DOC-ICP-09
[2]	**CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL**	DOC-ICP-08
[3]	**POLÍTICA DE SEGURANÇA DA ICP-BRASIL**	DOC-ICP-02
[4]	**REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP BRASIL**	DOC-ICP-10

5.2. Os documentos abaixo são aprovados por Instrução Normativa da ITI, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

5.3. Os documentos abaixo são aprovados pelo ITI, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br .

Ref	Nome do documento	Código
[6]	**Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE LABORATÓRIO DE ENSAIO E AUDITORIA**	ADE-ICP-10.07.A

ANEXO I

DOCUMENTOS PARA CREDENCIAMENTO DE LABORATÓRIO DE ENSAIO E AUDITORIA – LEA

O candidato a desenvolver as atividades de LEA deve entregar ao ITI os seguintes documentos atualizados:

1. Relativos a sua habilitação jurídica:

a) Ato constitutivo, devidamente registrado no órgão competente que comprove ser instituição brasileira, estabelecida há pelo menos 3 (três) anos, incumbida regimental ou estatutariamente de pesquisa em campo específico ou afim à segurança da informação e com inquestionável reputação ético-profissional;

b) Documentos da eleição de seus administradores, quando aplicável;

c) Documentos que comprovem ser instituição de pesquisa credenciadas pelo Comitê da Área de Tecnologia da Informação - CATI, Decreto Nº 5.906, de 26/09/2006, em conformidade com o disposto nas Resoluções por ele editadas, que estabeleçam os critérios para credenciamento de instituições para a execução de atividade de pesquisa e desenvolvimento, ou

d) Documento que comprove que o candidato está credenciado junto ao Sistema Brasileiro de Avaliação de Conformidade, conforme cadastro junto ao INMETRO.

2. Relativos a sua regularidade fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

3. Relativos a sua qualificação técnica:

A capacidade técnica e a capacidade de tratamento sigiloso de informações serão comprovadas por meio de realização de Auditoria Pré-Operacional e com base no ANEXO II - REQUISITOS MÍNIMOS DE SEGURANÇA PARA LABORATÓRIO DE ENSAIO E AUDITORIA

a) Política de Segurança - PS, atendendo às condições mínimas estabelecidas na

POLÍTICA DE SEGURANÇA DA ICP-BRASIL[3] no que couber;

b) Documentação que comprove a existência de pessoal qualificado, voltado ao objeto da avaliação de conformidade de sistemas e equipamentos de certificação digital, seja nos quadros do organismo, seja fora dele, e, nesta hipótese, deverá ser comprovada a vinculação contratual com o pessoal qualificado. O pessoal apresentado deve comprovar capacitação técnica para as finalidades da avaliação de conformidade quanto à formação profissional, experiência profissional e capacidade técnica, constantes de currículo Lattes devidamente cadastrado no CNPq, devendo, ainda, comprovar imparcialidade, independência e objetividade nas decisões; e

NOTA 1: Na hipótese do candidato já estar credenciado como LEA, em relação a outro sistema ou equipamento de certificação digital, desejando expandir o escopo de atuação, os documentos a serem apresentados, ficam restritos àqueles descritos no item 3, alínea "b". Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO II

REQUISITOS MÍNIMOS DE SEGURANÇA PARA LABORATÓRIOS DE ENSAIOS E AUDITORIA

1. DISPOSIÇÕES GERAIS

- Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos a serem adotados pelos Laboratório de Ensaio e Auditoria - LEA da ICP-Brasil.
- Suplementa, para essas entidades, os regulamentos contidos no documento **DOC-ICP-10 [4]**, tomando como base também a Política de Segurança da ICP-Brasil – **DOC-ICP-02 [3].**
- Os requisitos abaixo informados deverão ser apresentados quando do credenciamento do LEA e mantidos atualizados durante seu funcionamento enquanto entidade estiver credenciada na ICP-Brasil.
- O LEA deverá ter uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que devem ser seguidos em suas dependências e atividades, em consonância com o **DOC-ICP-02 [3].**
- Deverá existir um exemplar da Política de Segurança da Informação no formato impresso disponível para consulta no Nível 1 de segurança do LEA.
- A Política de Segurança da Informação deverá ser seguida por todo pessoal envolvido nos projetos coordenados pelo LEA, do seu próprio quadro ou contratado.
- Este documento define normas de segurança que deverão ser aplicadas nas áreas internas ao LEA assim como no trânsito de informações e materiais com entidades externas.
- A seguir são informados os requisitos que devem ser observados quanto a segurança de pessoal, segurança física, segurança lógica, segurança de rede, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios e análise de registros de eventos.

2. SEGURANÇA DE PESSOAL

- O LEA deverá ter uma Política de Gestão de Pessoas que disponha sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.
- A comprovação da capacidade técnica do pessoal envolvido nos projetos coordenados pelo LEA deverá estar a disposição para eventuais auditorias e fiscalizações.
- Todo pessoal envolvido nos projetos coordenados pelo LEA, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.
- O termo de sigilo da informação deverá conter cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos da ICP-Brasil.
- Aplica-se o termo de sigilo de informações a quaisquer outras entidades que porventura tenham acesso as informações internas e de terceiros originárias dos projetos coordenados pelo LEA.

- O LEA deverá ter procedimentos formais de apuração e responsabilização em caso de descumprimento das regras estabelecidas pelas suas políticas ou pelas normas da ICP-Brasil.
- O pessoal do LEA, e contratados, deverão possuir um dossiê contendo os seguintes documentos:
    a) contrato de trabalho ou cópia das páginas da carteira de trabalho onde consta o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;
    b) currículo Lattes devidamente cadastrado no CNPq;
    c) comprovante da verificação de antecedentes criminais;
    d) comprovante da verificação de situação de crédito;
    e) comprovante da verificação de histórico de empregos anteriores;
    f) comprovação de residência;
    g) comprovação de capacidade técnica;
    h) resultado da entrevista inicial, com a assinatura do entrevistador;
    i) declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir as regras aplicáveis da ICP-Brasil;
    j) termo de sigilo.
- Não são admitidos estagiários no exercício das atividades do LEA.
- Quando da demissão, o referido dossiê deverá possuir os seguintes documentos:
    a) evidências de exclusão dos acessos físico e lógico nos ambiente do LEA;
    b) declaração assinada pelo empregado ou servidor de que não possui pendências, conforme previsto no item 7.3.10 do DOC-ICP-02 [3].

3. SEGURANÇA FÍSICA

O ambiente físico do LEA deverá ser dividido em áreas claramente delimitadas, cada qual com diferentes requisitos de segurança, e organizada em níveis de segurança crescente.

O LEA deverá ter cinco níveis de segurança, resumidos na tabela abaixo:

Nível	Descrição
1	Atendimento
2	Operação
3	Sensível (Ambiente de Tecnologia da Informação e Ensaios)
4	Depósito
5	Depósito individual

Os níveis de segurança deverão ter seus pontos de acesso alinhados, de forma que os acessos a cada nível exijam acesso ao nível anterior.

As áreas físicas de cada um destes níveis de segurança deverão atender aos requisitos de segurança definidos para o respectivo nível.

3.1. Nível 1 - Atendimento

- O primeiro nível, ou nível 1, deverá situar-se após a primeira barreira de acesso às instalações do LEA.
- Os visitantes, para entrar em uma área de nível 1, deverão ter seu acesso autorizado por empregado do LEA com essa atribuição.
- Nenhum tipo de processo operacional ou administrativo do LEA, excetuando-se recebimento ou devolução de material de ensaio, deverá ser executado neste nível.

Excetuados os casos previstos em lei, o porte de armas não será admitido no nível 1 do LEA.

3.2. Nível 2 – Operação

- O segundo nível, ou nível 2, será interno ao primeiro. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo técnico operacional do LEA.
- Deverá existir um registro automático dos acessos das pessoas ao nível 2 informando o horário de entrada e o horário de saída.
- O acesso de pessoas ao segundo nível deverá ser restrito por uma porta com tranca.
- Os visitantes, poderão ter permissão de acesso concedida por empregado do LEA com essa atribuição
- Neste nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização e supervisão.

3.3. Nível 3 – Sensível

- No terceiro nível, ou nível 3, interior ao segundo, é onde deverão ocorrer as atividades especialmente sensíveis da operação do LEA.
- O acesso de pessoas ao nível 3 se dará por uma porta com autenticação automática (leitora de cartão ou biometria ou identificação de iris) e todos esses acessos deverão obrigatoriamente serem registrados.
- O acesso e permanência de visitantes neste nível será permitido somente quando autorizada e acompanhada por um empregado do LEA com essa atribuição.
- Todos os materiais inseridos e removidos do ambiente nível 3 também deverão ser registrados de forma automática (sistema de leitora código de barras ou similares).
- Telefones celulares, *tokens*, mídias de armazenamento, notebook, PDA, bem como outros equipamentos portáteis de comunicação e componentes sem-fio (*wireless*), exceto aqueles exigidos para a operação do LEA, não serão admitidos no nível 3.
- Poderão existir vários ambientes de nível 3, com as seguintes áreas:
    a) Ambiente de Tecnologia da Informação; e
    b) Laboratório de ensaios.

3.3.1. Ambiente de Tecnologia da Informação

- O Ambiente de Tecnologia da Informação deverá acomodar equipamentos como:
    a) Equipamentos de rede (*firewall*, roteadores, *switches* e servidores);
    b) Servidores do LEA (arquivos, correio eletrônico, etc.);
    c) Servidores de sistemas de segurança.
- Somente pessoas que necessitem realizar atividades de instalação, suporte ou manutenção de servidores, equipamentos e sistemas deverão ter permissão de acesso a este nível.

3.3.2. Laboratório de Ensaio

Nenhum ativo de ensaio deverá ser retirado do nível 3 exceto no momento de sua devolução ao solicitante de Laudo de Conformidade ou para os níveis 4 e 5 do próprio LEA**.**

3.4. Nível 4 – Sala depósito

- O quarto nível, ou nível 4, interior ao nível 3, refere-se a uma sala, um cofre ou um gabinete reforçado trancado.
- Ativos físicos de ensaio e ativos eletrônicos de ensaio armazenados em mídia removível deverão ser guardados em ambiente de nível 4 ou superior.
- Para garantir a segurança do material armazenado, a sala, o cofre ou o gabinete deverá possuir tranca com chave.
- O nível 4 deverá possuir os mesmos controles de acesso do nível 3 a cada acesso ao ambiente, recomendando-se o uso de biometria.
- Deverá existir um livro de acesso, ou aplicativo destinado a esse fim, no qual deverá ser registrado o motivo do acesso ao nível.

3.5. Nível 5 – Depósito individual

O quinto nível, ou nível 5, interior ao ambiente de nível 4, poderá ser composto de dois tipos de depósitos, de acordo com o tipo de ativo armazenado:

a) Depósito físico: deverá consistir de pequenos depósitos localizados no interior do nível 4. Cada um desses depósitos deverá dispor de fechadura individual. Deverá existir um livro-ata de custódia de material, individual para cada depósito, no qual deverão constar os itens retirados ou devolvidos e o motivo da transferência;
b) Depósito eletrônico: deverá consistir de uma hierarquia de diretórios ou arquivos individuais protegidos com criptografia (envelope digital). O servidor que hospeda tais depósitos deverá estar localizado em um ambiente nível 3. Associado a cada depósito eletrônico deverá existir um livro de acesso a material, no qual deverão constar os itens acessados e o motivo do acesso.

3.6. Disposições Gerais de Segurança Física

- O ambiente físico do LEA deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos.
- O LEA deverá conter imagens que garantam a identificação de pessoas quando do acesso

físico em qualquer parte de seu ambiente.

- É mandatório o sincronismo de data e hora entre os mecanismos de segurança física garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem.
- Todos que transitam no ambiente físico do LEA deverão portar crachás de identificação, inclusive os visitantes.
- Só é permitido o trânsito de material de terceiros pelos ambientes físicos do LEA mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação.
- O LEA deverá conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico.
- Todo material crítico inservível, descartável ou não mais utilizável deverá ter tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção deverá ter seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do LEA.
- Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, deverão estar inventariados com informações que permitam a identificação inequívoca.
- Em caso de inoperância dos sistemas automáticos, o controle de acesso físico deverá ser realizado provisoriamente por meio de um livro de registro onde constará quem acessou, a data, hora e o motivo do acesso.
- Deverão ser providenciados mecanismos para garantir a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote.

4. SEGURANÇA LÓGICA

- O acesso lógico ao ambiente computacional do LEA se dará no mínimo mediante usuário individual e senha, que deverá ser trocada periodicamente.
- Todos os equipamentos do parque computacional deverão ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas.
- Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa.
- O LEA deverá ter explícita a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários deverão estar cadastrados em perfis de acesso que permitam privilégio mínimo para realização de suas atividades.
- Os usuários especiais (a exemplo do *root* e do *administrator*) de sistemas operacionais, de banco de dados e de aplicações em geral devem ter suas senhas segregadas de forma que o acesso lógico a esses ambientes se dê por pelo menos duas pessoas autorizadas.
- Todo equipamento do LEA deverá ter *log* ativo e seu horário sincronizado com uma fonte confiável de tempo.
- As informações como *log*, trilhas de auditoria, registros de acesso (físico e lógico) e imagens deverão ter cópia de segurança cujo armazenamento será de 5 anos.
- Os softwares dos sistemas operacionais, os antivírus e aplicativos de segurança devem ser

mantidos atualizados.

5. SEGURANÇA DE REDE

- O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos.
- Não podem ser admitidos acessos do mundo externo a rede interna do LEA. As tentativas de acessos externos devem ser inibidas e monitoradas por meio de aplicativos que criem barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão.
- Devem ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada 3 meses. Os testes na rede devem ser documentados e as vulnerabilidades detectadas corrigidas.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

- Toda informação gerada e custodiada pelo LEA deverá ser classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação.
- A classificação da informação no LEA deverá ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada.
- A informação poderá ser classificada em:
    a) **Público**: Qualquer ativo de informação, de propriedade do LEA ou não, que poderá vir ao público sem maiores conseqüências danosas ao funcionamento normal do LEA. Poderá ser acessado por qualquer pessoa, seja interna ou externa ao LEA. Integridade da informação não é vital.
    b) **Pessoal**: Qualquer ativo de informação relacionado à informação pessoal. Por exemplo: mensagem pessoal de correio eletrônico, arquivo pessoal, dados pessoais, etc.
    c) **Interna**: Qualquer ativo de informação, de propriedade do LEA ou não, que não seja considerada pública. Ativo de informação relacionado às atividades do LEA que é direcionada estritamente para uso interno. A divulgação não autorizada do ativo de informação poderia causar impacto à imagem do LEA. Por exemplo: código fonte de programa, cronograma de atividades, atas de reuniões, etc.
    d) **Confidencial**: Qualquer ativo de informação que seja crítico para as atividades do LEA em relação ao sigilo e integridade. Qualquer material e informação recebida para ensaio, assim como qualquer resultado do ensaio (como relatório) deverá ser considerado confidencial.

Caso o LEA seja entidade da Administração Pública Federal - APF, aplicar-se-a as disposições do Decreto nº 4.553/2002 e demais normas aplicáveis à APF, no que couber.

7. SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

- O LEA deverá, em sua Política de Segurança da Informação, definir como será realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado "backup".
- A salvaguarda de ativos da informação deverá ter descrita as formas de execução dos seguintes processos:
    a) procedimentos de *backup*;
    b) indicações de uso dos método de *backup*;
    c) tabela de temporalidade;
    d) local e restrições de armazenamento e salvaguarda em função da fase de uso;
    e) tipos de mídia;
    f) controles ambientais do armazenamento;
    g) controles de segurança.
    h) teste de restauração de backup.
- O LEA deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

8. GERENCIAMENTO DE RISCOS

O LEA deverá ter um processo de gerenciamento de riscos, atualizado, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados atualizado, no mínimo, anualmente.

9. PLANO DE CONTINUIDADE DE NEGÓCIOS

Um Plano de Continuidade do Negócio – PCN deverá ser implementado e testado no LEA, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.

10. ANÁLISES DE REGISTROS DE EVENTOS

Todos os registros de eventos (logs, trilhas de auditorias e imagens) devem ser analisados, no mínimo, mensalmente e um relatório deverá ser gerado com assinatura do responsável pelo LEA.